ASKING THE RIGHT QUESTIONS ABOUT WAR EXCLUSIONS IN THE CONTEXT OF CYBER OPERATIONS

Anthony Cordonnier
Global Co-Head of Cyber,
Guy Carpenter

Erica Davis
Global Co-Head of Cyber,
Guy Carpenter

Michael Sevi
General Counsel,
Guy Carpenter

In the last several years, reinsurance and insurance markets have grappled with the meaning of the war exclusion in the context of cyberattacks (or more broadly “cyber operations”). The ongoing Russian invasion of Ukraine, including cyber operations that crashed websites of Ukraine’s defense ministry and two large Ukrainian banks, underscores the need for contract certainty regarding coverage for state-sponsored cyber operations. Yet, legal guidance on the application of the war exclusion to cyber operations remains elusive. The recent court decision in *Merck v. Ace American Insurance Company et al.*, the first to consider whether a war exclusion applies to a cyber operation, does not provide meaningful answers.

We suggest that stakeholders ask new questions. Over the last year-and-a-half, the Geneva Association, in collaboration with the International Forum of Terrorism Risk (Re)Insurance Pools (jointly referred to here as the Geneva Association), and Lloyd’s Market Association (LMA) have suggested better ways to think about—and clarify—coverage for state-sponsored cyber operations. This article explains the problems posed by traditional war exclusions in the cyber context and how recently-drafted clauses, which markets have increasingly adopted, address these problems. We then consider reinsurance implications.

Traditional Questions of Attribution and Characterization

A war exclusion, as used in both standalone cyber policies and general property and liability policies, excludes losses caused by “war” or “warlike” actions. Wordings vary, but in practice, the exclusion turns on two key questions: first, is the loss-causing conduct attributable to a sovereign state? Second, is the loss-causing conduct properly characterizable as “warlike”? These questions create substantial uncertainty in the context of cyber operations.

Identifying the perpetrator of a cyber operation is challenging, costly and inexact. Governments are best positioned to identify perpetrators, but they may not do so publicly. If a government does make a public attribution, its assessment may be influenced by diplomacy, politics and even insurance implications. Further, different governments may take opposing positions on the attribution of a cyber operation.

Once a perpetrator is identified, the relationship between the perpetrator and the relevant state must be determined, which presents another challenging factual issue. Even assuming all the facts are known, a difficult question remains: What kind of state involvement is sufficient to attribute a cyber operation to the state? The wording of a war exclusion may provide little guidance.

It is equally uncertain whether courts will characterize cyber operations as warlike conduct under existing legal precedents governing kinetic warfare. The traditional factors—such as the proximity of a cyber operation to a "theater of war," the presence of uniformed, weapon-carrying combatants, and the use of physical force—are ill-suited to determine whether a state-sponsored cyber operation is "warlike." A cyber operation can serve a state's military or diplomatic goals without physical force—for example, through espionage or data theft.

The first court decision analyzing the application of the war exclusion to a cyber operation, *Merck v. Ace American Insurance Company et al. (New Jersey Superior Court, Jan. 2022)*, provides little insight on these core questions of attribution and characterization.

Merck v. Ace American Insurance et al. Does Not Provide Clear Answers

In June 2017, on the eve of Ukraine's Constitution Day, NotPetya malware infiltrated the software of a small Ukrainian firm and then spread to digital media in other countries. NotPetya caused an estimated USD 10 billion of losses, including over USD 1.4 billion claimed by Merck. In 2018, the US publicly attributed the malware to the Russian military. NotPetya was launched in the context of intermittent armed conflict between the Ukrainian military and Russian separatist forces in Eastern Ukraine, which had resulted in thousands of civilian deaths since Russia annexed Crimea in 2014.

Merck had standalone cyber coverage, but the severe damage caused by NotPetya left it underinsured. Accordingly, Merck pursued a separate claim under its "all-risk" property policies. The insurers denied the claim, citing the policies' war exclusion, which excluded losses caused by "hostile or warlike action" by an "agent" of a "government." In response, Merck filed suit in New Jersey state court.

In its decision, the court avoided the questions of attribution (was the Russian government responsible for the cyber operation?) and characterization (was the cyber operation warlike conduct?) by stacking the deck against Merck's insurers. The court invoked a technical principle of contract law called *contra proferentum*, which means that ambiguities in an exclusion should be resolved against the insurer and in favor of finding coverage. The court ruled that the war exclusion did not apply unless Merck's interpretation of the exclusion was "entirely unreasonable."

Measured against this high standard, the court "unhesitatingly" concluded that the war exclusion did not apply because no court had ever applied a war exclusion to "anything remotely close" to a cyber operation. According to the court, if the insurers wanted the exclusion to extend beyond "traditional forms of warfare," they should have clarified their policy language.

MERCK HAD STANDALONE CYBER COVERAGE, BUT THE SEVERE DAMAGE CAUSED BY NOTPETYA LEFT IT UNDERINSURED.

The court's reasoning is questionable. The New Jersey Supreme Court has held that the principle of *contra proferentum* does not apply to a sophisticated commercial insured like Merck. Additionally, the court did not explain why the broad language of the exclusion—"hostile" acts by a government "agent"—did not encompass cyber operations. Finally, the court ignored the fact that the NotPetya operation took place in the context of traditional forms of warfare in Eastern Ukraine. The decision sheds little light on questions of attribution and characterization of cyber operations. The Appellate Division of the New Jersey Superior Court granted the insurers permission to immediately appeal the ruling, signaling the importance of the issue and the need for clear guidance from a higher court.

The other closely watched case where an insurer invoked the war exclusion to deny cover for NotPetya losses, *Mondelez International v. Zurich American Insurance Company (Cook County Circuit Court)*, recently settled during trial. Thus, even after the *Merck* case is resolved, guidance on the application of the war exclusion to cyberattacks will exist in only one US jurisdiction.

Asking Better Questions

The Merck decision looks backwards to an "all risk" property policy written in 2017. However, market participants have made important improvements to cyber cover in the last 5 years. Exposure to "silent cyber" in general property and liability policies—like the policies at issue in the *Merck v. Ace et al.* case—has been limited through explicit exclusions, affirmative coverage and sub-limits. Additionally, the war exclusion in standalone cyber policies often includes a carve-back for cyberterrorism, even when committed by a state actor.

Progress has also been made on the questions of attribution and characterization. With respect to attribution, industry groups have refined the need for state involvement. To streamline the analysis, the LMA's model "Cyber War and Cyber Operation Exclusion Clauses" create a rebuttable presumption that an attribution by the government of the affected country is determinative. Meanwhile, the Geneva Association suggests a "spectrum of state responsibility" ranging from state-ignored conduct to state-executed conduct. Specific language regarding state involvement can reduce contract uncertainty.

More significant advances have been made with regard to characterization. The Geneva Association urges market participants to address whether coverage applies to "hostile cyber activity"—state-sponsored cyber operations that fall short of "war" or "warlike" conduct. LMA's new cyber exclusions implement this approach. They are organized around the term "cyber operation," which means "use of a computer system by or on behalf of a state to disrupt, deny, degrade, manipulate or destroy information in a computer system of or in another state." This definition of "cyber operation" avoids the characterization question, as a policy can cover or exclude all cyber operations attributable to a state—regardless of whether they are "warlike."

Of course, reinsurers and insurers may seek to limit coverage for state-sponsored cyber operations that have the potential for large, correlated losses. LMA exclusions try to provide flexibility in 2 ways. First, the model exclusions apply to cyber operations that have a "major detrimental impact" on the "functioning of a state" by impairing an "essential service" or the "security or defen[s]e of a state." NotPetya, while harmful to Merck and other companies, did not impair an essential service vital to the functioning of a country. If NotPetya had triggered a widespread power outage, or disrupted a large proportion of a country's food supply, this type of exclusion could apply. Second, the exclusions apply to a "cyber operation that is carried out in the course of war"—that is, a cyber operation that is part of traditional kinetic warfare.

AS CYBER EXCLUSIONS EVOLVE, CEDENTS MUST CONFIRM THAT THEIR REINSURANCE CONTRACTS PROVIDE ADEQUATE COVER.

The approaches suggested by the Geneva Association and LMA raise new questions. What level of "state responsibility" is sufficient for attribution? What is the threshold for an excluded cyber operation that impairs an "essential service" or the "functioning of a state"? But these are better questions—they form part of an ongoing dialogue to clarify coverage for cyber operations and to separate the insurable from the uninsurable.

Further, these questions can no longer be avoided. In August 2022, LMA issued a bulletin requiring managing agents to adopt contract language that addresses these questions in standalone cyber policies. Specifically, wordings must provide a “robust basis” to determine attribution, exclude cyber operations that significantly impair the functioning or security capabilities of state, and declare whether coverage exists outside a country whose functioning or security capabilities are substantially impaired by a cyber operation. Wording amendments to help clarify these issues are already being circulated in the market, and we expect the LMA to refine its guidance in response. Ultimately, this dialogue will help create a stronger market for cyber insurance.

Reinsurance Implications

As cyber exclusions evolve, cedents must confirm that their reinsurance contracts provide adequate cover. Many reinsurance treaties have war exclusions that apply “as per the Company’s original policy,” or similarly, state that they are inapplicable to original policies with a “War Exclusion Clause.” These provisions create back-to-back coverage—i.e., if the war exclusion in the insurer’s policy does not apply, then the reinsurer’s war exclusion will not apply either. Other treaties have a war exclusion that applies when the underlying policy does not have a war exclusion. Still other treaties have a war exclusion that applies without regard to a war exclusion in the underlying policy. The latter two scenarios can create a gap in reinsurance cover and should be treated with the utmost care.

As the dialogue prompted by the Geneva Association and LMA progresses, language in original policies is evolving rapidly and reinsurance contracts need to adapt. Accordingly, cedents should monitor whether exclusions in their reinsurance contracts remain “back to back” with any cyber exclusions in their policies. Otherwise, losses from a cyber operation could be covered by an underlying policy but excluded from a reinsurance contract.

How Guy Carpenter Helps Clients

Guy Carpenter’s Global Cyber team of brokers, contract consultants, product innovators and analytic experts assists clients with cyber reinsurance needs, including analysis of emerging model wordings, silent cyber stress tests, and scenario modeling for numerous historic and potential threats. As the need to carefully review and consider the shifting wordings of war exclusions grows daily, Guy Carpenter is helping our clients ask the right questions to maximize the value of their cyber reinsurance coverage.

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with 3,400 professionals in over 60 offices around the world. Guy Carpenter delivers a powerful combination of broking expertise, trusted strategic advisory services and industry-leading analytics to help clients adapt to emerging opportunities and achieve profitable growth. Guy Carpenter is a business of Marsh McLennan (NYSE: MMC), the world’s leading professional services firm in the areas of risk, strategy and people. The Company’s 86,000 colleagues advise clients in 130 countries. With annual revenue of over $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses including Marsh, Mercer, and Oliver Wyman. For more information, visit www.guycarp.com and follow us on LinkedIn and Twitter @GuyCarpenter.

Guy Carpenter & Company, LLC provides this report for general information only. The information contained herein is based on sources we believe reliable, but we do not guarantee its accuracy, and it should be understood to be general insurance/reinsurance information only. Guy Carpenter & Company, LLC makes no representations or warranties, express or implied. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. Statements concerning tax, accounting, legal or regulatory matters should be understood to be general observations based solely on our experience as reinsurance brokers and risk consultants, and may not be relied upon as tax, accounting, legal or regulatory advice, which we are not authorized to provide. All such matters should be reviewed with your own qualified advisors in these areas.

Readers are cautioned not to place undue reliance on any historical, current or forward-looking statements. Guy Carpenter & Company, LLC undertakes no obligation to update or revise publicly any historical, current or forward-looking statements, whether as a result of new information, research, future events or otherwise. The trademarks and service marks contained herein are the property of their respective owners.